Satellite Network Security

Marlyn Kemper Littman
Nova Southeastern University, USA

INTRODUCTION

Satellite networks play a vital role in enabling essential critical infrastructure services that include public safety; environmental monitoring; maritime disaster recovery and reconnaissance; electronic surveillance; and intelligence operations for law enforcement, the military, and government agencies (Jamalipour & Tung, 2001). As demonstrated by the events following the terrorist attacks in the U.S. on the Pentagon in Washington, D.C. and the World Trade Center in New York City on September 11, 2001, satellite networks also provide redundant communications services when terrestrial networks are disrupted and/or unavailable. Despite their merits, satellite networks are nonetheless vulnerable to cyber attacks that pose threats to national security and the economy.

Satellite networks transport voice, video, images, and data through the air as electromagnetic signals, thereby making these transmissions susceptible to interception. Technical advances enable the interconnectivity of satellite systems to public and private wireless and terrestrial networks including the Internet. These advances, however, amplify the risk of cyber attacks that can compromise critical infrastructure functions dependent on satellite networks in sectors that include information technology (IT) and telecommunications; defense; government; banking and finance; utilities; agriculture; emergency services; public health; and transportation (U.S. Department of Homeland Security (DHS), 2003; U.S. Government Accounting Office (GAO), 2004). As a consequence, satellite networks employ an array of security tools and mechanisms for countering costly and widespread cyber incursions and, thereby, ensuring the continuity of critical infrastructure operations. Those cyber attacks that are politically motivated and specifically designed to disrupt essential services are generally attributed to *cyber terrorism*.

This chapter describes the technical fundamentals of satellite networks; examines security vulnerabilities; and explores initiatives for protecting the integrity of satellite network transmissions and operations from cyber incursions and physical attacks. Standards and protocols that safeguard satellite networks from unauthorized use and intentional disruptions and policies, and legislation that facilitate cyberspace asset protection are described. Capabilities of *encryption* in supporting secure satellite services and the distinctive attributes of the InterPlanetary Internet (IPN), also called the InterPlanetary Network**,** are explored.

BACKGROUND

Satellite Network Technical Fundamentals

Satellite networks consist of ground and space segments. The ground segment includes a ground or earth station that delivers communications services and monitors satellite operations by providing tracking, telemetry, and control (TT&C) functions. The space segment consists of the artificial satellite and its payload.

In contrast to a natural satellite or a celestial body that revolves around a larger sized planet, an artificial satellite is a wireless receiver/transmitter that orbits the earth and employs microwave technology in the super high and extremely high radio frequency (RF) bands of the electromagnetic spectrum to enable wide area interactive communications (Littman, 2002). The payload includes transceivers and antennas for RF signal reception, amplification, and retransmission.

The quality of the satellite signal reflects the quality of the uplink and downlink. An uplink describes signal transmissions from an earth station such as a gateway, teleport, hub, or very small aperture terminal (VSAT) to the satellite. A downlink refers to signal transmissions from the satellite to the designated reception site. Typically, satellite transmissions are asymmetrical with more information transported on the downlink than on the uplink (Littman, 2002). Generally classified in terms of the orbits in which they operate, satellite constellations are categorized as geosynchronous or geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO).

Satellite Network Vulnerabilities

Satellites' transmissions are subject to lengthy delays, low bandwidth, and high bit-error rates that adversely impact real-time, interactive applications such as videoconferences and lead to data corruption, performance degradation, and cyber incursions. Atmospheric and interstellar noise; cosmic radiation; interference from electronic devices; and precipitation and rain absorption in the spectral frequencies employed

by satellites impede network performance and information throughput and negatively affect provision of quality of service (QoS) guarantees (Littman, 2002).

Satellite network applications and services are also adversely impacted by geophysical events. In 1998, for example, tremendous explosions on the sun disrupted operations onboard PanAmSat's Galaxy IV Satellite. As a consequence of these solar flares, digital paging services, bank transactions, and cable television programs across the U.S. were disabled (U.S. GAO, 2002).

According to the U.S. GAO (2002), satellite network functions can be compromised by ground-based antisatellite weapons, high-altitude nuclear explosions, stealth micro satellites, space mines, space-to-space missiles, and directed energy space weapons. For instance, as a consequence of intentional jamming resulting from cyber attacks on a Telestar-12 commercial satellite in 2003, U.S. government-supported broadcasts promoting regime changes in Iran were blocked by the Iranian Ministry of Post, Telegraph, and Telephone (Waldrop, 2005). Satellite-based telephony services in Tehran were also disabled.

Satellite network operations are subject to denial of service (DoS) and distributed DoS (DDoS) attacks generated by automated tools that prevent authenticated users from accessing network services; the spread of viruses to mobile satellite-enabled appliances such as cellular phones; worms that self-propagate malicious data; and spy ware that enables intruders to gain unrestricted access to classified documents (U.S. GAO, 2005) as well. denial of information (DoI) attacks on satellite networks such as spam or unsolicited commercial e-mail and phishing or transmission of fraudulent e-messages are typically designed to deceive legitimate users into revealing confidential information to unauthorized sources (Conti & Ahamad, 2005; Wilson, 2005).

Satellite networks are also vulnerable to cyber terrorism or coordinated space-based and ground-based threats and attacks committed by unlawful and/or politically motivated terrorist groups who target critical communications systems such as satellite networks to cause data corruption, disruption of critical infrastructure services, economic damage, harm, and loss of life (Wilson, 2005). Satellite network attacks attributed to cyber terrorism can result in disruptions in financial markets and disclosure of government, law enforcement, medical, and/or military classified data (U.S. GAO, 2004). Intentional satellite system incursions motivated by cyber terrorism raise questions about the dependability, reliability, availability, and security of satellite network services and erode public confidence in the integrity of satellite-dependent, critical infrastructure applications (Bosch, 2002).

SATELLITE NETWORK SECURITY INITIATIVES

A multifaceted approach with multiple levels of security is required to protect satellite networks against cyber attacks that can culminate in malicious data corruption; system and service disruptions; unauthorized information disclosure; and physical destruction of satellite assets. Implementation of procedures for safeguarding satellite space and ground segments, TT&C functions, and satellite uplink and downlink transmissions; strategies to optimize satellite network performance; and satellite security protocols to provide authentication and authorization services must be based on a systematic assessment of satellite network risks and a comprehensive determination of satellite network security requirements (Roy-Chowdhury, Baras, Hadjitheodosiou, & Rentz, 2005). Tools, procedures, and measures that aid in safeguarding satellite operations include the enactment of public policies and legislation; the implementation of satellite security protocols and standards; and the utilization of security mechanisms and tools such as encryption.

Public Policies and Legislation

Presidential Decision Directives Nos. 49 (1996) and 63 (1998) define U.S. satellites' space activities as critical to national defense, economic security, and public health and safety and are essential in supporting critical infrastructure protection. U.S. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No.12 establishes a foundation for a nationwide information assurance policy to guide the planning, design, implementation, and operations of secure U.S. space systems (NSTISSC, n.d.). NSTISSP No. 12 measures also mandate that U.S. space systems support information confidentiality, data integrity, user authentication, the availability of information services to authorized users, and service nonrepudiation. Empowered by the U.S. Homeland Security Act of 2002, the U.S. DHS supports comprehensive vulnerability assessments and coordinates nationwide response to threats and attacks classified as cyber terrorism in conjunction with entities that include the U.S. National Infrastructure Protection Center (U.S. DHS, 2003).

International cyber security agreements and public policies such as the Council of Europe's Convention on Cybercrime endorsed in 2001 by 38 countries including the U.S. promote development of international legislation to deter cyber terrorism activities (Wilson, 2005). In 2003, a joint declaration of Cooperation to Combat Terrorism supported by the European Union and the Association of South East Asian Nations (ASEAN, 2003) called for international cooperation in detecting and responding to threats of attacks on satellite assets.

SATELLITE STANDARDS AND PROTOCOLS

Space Communication Protocol Standards

Developed by the Consultative Committee for Space Data Systems (CCSDS), an international consortium that includes space agencies in countries such as Japan, Canada, and the U.S. among its membership, CCSDS establishes the Space Communication Protocol Standards (SCPS) to promote space system interoperability and security. The SCPS suite is based on the Transmission Control Protocol/Internet Protocol (TCP/IP) specifications that also serve as the foundation for the public or commodity Internet. Endorsed by the International Organization for Standardization (ISO) in 1999, the SCPS suite defines approaches for space data transmissions; secure communications to and from space and ground segments; and satellite information management (Hooke, 2001).

The CCSDS SCPS-File Protocol (SCPS-FP) describes processes for error recovery, access control, and privacy. Developed for the U.S. National Aeronautics Space Agency (NASA) Mercury, Surface, Space Environment, Geochemistry, and Ranging (MESSENGER) mission in 2004, the CCSDS-File Delivery Protocol (CCSDS-FDP) , also known as CFDP, supports dependable and secure file transfers across interplanetary distances and standardized file downlink operations between satellites and ground stations (Krupiarz et al., 2002). CFDP uses forward error correction coding to detect data loss and request retransmission.

The SCPS-Transmission Protocol (SCPS-TP) employs algorithms to control data loss resulting from congestion and signal corruption (CCSDS, 1999). Performance enhancing proxies (PEPs) such as TCP spoofing algorithms optimize SCPS-TP operations by enabling header compression, dynamic buffering, and reliable and fast transmissions.

Based on the Integrated-Network Layer Security Protocol (I-NLSP) and the Internet Protocol Security (IPsec) Encapsulation Security Header (ESH) and Authentication Header (AH) protocols, the SCPS-Security Protocol (SCPS-SP) supports data confidentiality; access controls for space operations with minimal overhead; and data protection, authentication, and authorization services (CCSDS, 1999). SCPS-SP encapsulates transport protocol data units (TPDUS) into secure protocol data units (SPDUS) to maintain integrity of space transmissions. It is important to note that SCPS-SP does not recommend the use of specific cryptographic algorithms or key management systems since these functions are handled by the Data-Link Layer or Layer 2 and the Physical Layer or Layer 1 of the seven-layer Open Systems Interconnection (OSI) Reference Model.

Satellite Internet Protocol Security (SatIPSec)

Endorsed by the Internet Engineering Task Force (IETF) and based on IPSec**,** SatIPSec facilitates secure IP unicast transmissions between a single sender and a single receiver and multicast transmissions between a single sender and a multiple group of receivers. In addition to working with IPv4 (IP version 4) and IPv6 (IP version 6), SatIPSec safeguards satellite network operations that are vulnerable to threats and incursions ranging from satellite terminal cloning to eavesdropping (Duquerroy, Josset, Alphand, Berthou, & Gayraud, 2004). SatIPSec maintains data integrity through the use of symmetric encryption that enables authorized multicast group members to verify the origin, identity, and source of multicast transmissions.

Satellite-Reliable Multicast Transport Protocol

Satellite-Reliable Multicast Transport Protocol (SAT-RMTP) was developed by the University of Aberdeen (n.d.) and endorsed by the IETF, SAT-RMTP enables reliable transport and delivery of multimedia files and video clips via GEO satellite constellations to terrestrial networks. Capabilities of SAT-RMTP were verified in tests supported by GEOCAST (Multicast over Geostationary Extremely High Frequency [EHF] Satellites), a European Commission Information Society Technologies (IST) initiative.

Security Tools and Mechanisms

Satellite network security operations are supported by an array of satellite tools and mechanisms ranging from antivirus software and stateful firewalls to attack-resistant or hardened satellite components and physical and logical access controls requiring the use of devices such as smart cards and biometric systems that employ retinal scans and fingerprints for authentication. Redundant security systems for surveillance and fire, flood, and windstorm protection safeguard satellite ground station operations from deliberate cyber attacks, unauthorized use, and natural and artificial disasters.

In the U.S., the Department of Defense Advanced Research Projects Agency (DARPA) is evaluating the security capabilities of pseudolites or pseudo satellites that support redundant communications services if ground station equipment is deliberately disabled. The U.S. Air Force employs antijamming units to safeguard ground station operations; outbound filters to prevent forged source addresses from infiltrating satellite systems; and space telescopes to monitor space activities classified as cyber terrorism. The U.S. Air Force also supports development of sophisticated high-power

space weapons equipped with laser beams to temporarily disable adversary satellites attempting to deny the U.S. utilization of its own space network (U.S. DHS, 2003).

A popular satellite network security tool—encryption—enables safe transmissions via insecure satellite uplinks and downlinks. Conventional encryption systems employ algorithms to scramble plaintext into ciphertext or a meaningless format prior to transmission (Littman, 2002). A key or a secret piece of information typically consisting of a string of random bits enables decryption and the restoration of the message to plaintext or its original format. Digital signatures and time stamps are used in conjunction with encryption to authenticate message integrity. In asymmetric cryptosystems, a public key that is shared by two or more individuals supports encryption, and a private key known only to the message recipient facilitates decryption. In symmetric cryptosystems, the same public key is used for encryption and decryption.

In the absence of strong encryption, cyber intruders can compromise satellite operations by eavesdropping and conducting brute force attacks of weakly encrypted data. In 2002, for instance, unauthenticated subscribers to satellite television programming in the European Union viewed unencrypted surveillance video of U.S. military bases in Bosnia when the cryptosystem was compromised. Satellite television providers generally use conventional encryption systems that employ mathematical algorithms for decryption to ensure that only subscribers with authorized receivers can decrypt television signals and receive delivery of television and pay-per-view entertainment programs. In accordance with NSTISSP No. 12 (NSTISSC, n.d.), U.S. space systems must employ robust encryption to safeguard command and control data and national security information transported between satellite space and ground segments.

The U.S. Army provides access to classified and unclassified information and support services to field units in Iraq via the Combat Service Support Satellite Communications VSAT network. This network employs Triple Digital Encryption Standard (3DES) and complies with the Federal Information Processing Standard (FIPS) 140-2 that specifies security requirements for cryptographic modules. Since 3DES and its forerunner DES are susceptible to hacker attacks, the U.S. National Institute of Standards and Technology (NIST) recommends their replacement by Advanced Encryption Standard (AES), a block cipher encryption algorithm that is unclassified, available without royalty charges worldwide, and complies with FIPS 197 (Burr, 2003). Also called the Rijndael block cipher after its developers Vincent Rijmen and Joan Daemen, AES uses 128-bit, 192-bit, and 256-bit encryption keys.

FUTURE TRENDS

Established by DARPA as a state-of-the-art, next-generation, Internet initiative, the IPN is a deep space backbone network that features a delay-tolerant network (DTN) architecture capable of operating in terrestrial and interplanetary environments with minimal bandwidth, limited power, high error rates, and latencies or delays in the length of time required for information transport from source to destination (Akyildiz, Akan, Chen, Fang, & Su, 2004). The IPN is designed to interlink terrestrial networks including the Internet with remotely located Internets on other planets or spacecraft in transit. Based on CFDP, the IPN bundle layer consists of a delay-tolerant protocol stack that complements DTN architecture. By supporting store-and-forward operations, the bundle layer relays voice, video, image, and data message fragments as bundles from heterogeneous networks via IPN nodes for secure transmission when forward links are established (Burleigh et al., 2003). The store-and-forward operations accommodate uncertain and intermittent interconnectivity between IPN nodes and lengthy propagation delays associated with space-based transmissions. Importantly, the bundling layer also supports the use of multiple data-protection mechanisms to ensure the security of IPN backbone operations and the integrity of information transmitted and exchanged across interplanetary distances in harsh space environments (Hooke, 2001).

Since deep space missions may not have direct line of sight between the earth and the final destination address, IPN bundles may also be transported to recipient locations via satellites that function as intermediate IPN nodes (Akyildiz et al., 2004). Approaches for ensuring secure and reliable IPN transmissions, protecting IPN infrastructure operations from cyber attacks, and utilizing access controls and authentication mechanisms to ensure bundle integrity and data privacy are in development.

CONCLUSION

Satellite network security is dependent on carefully designed and effectively implemented security tools, mechanisms, standards, and protocols; policies and legislation; and procedures that prevent unauthorized entities from gaining access to ground stations; eavesdropping on confidential satellite transmissions; altering satellite information in transit; falsifying command and control data; and destroying satellite assets (Roy-Chowdhury et al., 2005). Even when multiple security devices and countermeasures are in place, however, satellite networks remain vulnerable to ground-based and space-based attacks. The mounting incidents of satellite network cyber incursions attributed to cyber terrorism and the potentially

adverse impacts of these attacks on critical infrastructure operations underscore the importance of building secure satellite networks to protect the integrity, reliability, sustainability, and availability of critical infrastructure resources, services, and initiatives.

REFERENCES

Akyildiz, I., Akan, O., Chen, C., Fang, J., & Su, W. (2004). The state of the art in interplanetary Internet. *IEEE Communications Magazine, 42*(7), 108-118.

ASEAN (2003). *Joint declaration on cooperation to combat terrorism*. Retrieved June 27, 2006, from http://www.aseansec.org/14030.htm

Bosch, O. (2002). Cyberterrorism and private sector efforts for information infrastructure protection. *Creating Trust in Critical Networks. Workshop of the ITU Strategy and Policy Unit*. Retrieved November 15, 2005, from http://www.itu.int/osg/spu/ni/security/workshop/presentations/cnibosch paper.doc

Burleigh, S., Cerf, V., Durst, R., Fall, K., Hooke, A., Scott, K. et al., (2002, Oct. 10-19). The interplanetary Internet: A communications infrastructure for Mars exploration. *53rd International Astronautical Congress: The World Space Congress,* Houston, TX.

Burr, W. E. (2003). Selecting the advanced encryption standard. *IEEE Security & Privacy Magazine, 1*(2), 43-52.

Consultative Committee for Space Data Systems (CCSDS). (1999). *Report on the application of CCSDS protocols to secure systems*. Retrieved November 30, 2005, from http://telecom.esa.int/telecom/www/object/index.cfm?fobjectid=11703

Conti, G., & Ahamad, M. (2005). A framework for countering denial-of-information attacks. *IEEE Security & Privacy Magazine, 3*(6), 50-56.

Duquerroy, L., Josset, S., Alphand, O., Berthou, P., & Gayraud, T. (2004, May 9-12). Satellite Internet Protocol Security (SatIPSec): An optimized solution for securing multicast and unicasts satellite transmissions. *Twenty-second American Institute of Aeronautics and Astronautics (AIAA) International Communications Satellite Systems Conference (ICSSC) and Exhibit,* Monterey, CA.

Hooke, A. (2001). The interplanetary Internet. *Communications of the ACM, 44*(9), 38-40.

Jamalipour, A., & Tung, T. (2001). The role of satellites in global IT: Trends and implications. *IEEE Personal Communications, 8*(3), 5-11.

Krupiarz, C., Burleigh, S., Frangos, C., Heggestad, B., Holland, D., Lyons, K. et al. (2002). The use of the CCSDS file delivery protocol on MESSENGER. *NASA SpaceOps 2002 Conference Papers*. Retrieved October 8, 2005, from http://www.spaceops2002.org/papers/SpaceOps02-P-T5-35.pdf

Littman, M. K. (2002). *Building broadband metworks.* Boca Raton, FL: CRC Press.

National Security Telecommunications and Information Systems Security Committee (NSTISSC). (n.d.). Fact sheet. NSTISSP No. 12. National information assurance (IA) policy for U.S. space systems. Retrieved June 27, 2006, from www.cnss.gov/Assets/pdf/nstissp_12.pdf

Presidential Decision Directive 49. (1996, September 19). *Fact sheet—National space policy.* Retrieved June 1, 2006, from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

Presidential Decision Directive 63. (1998, May 22). *Fact sheet—Critical infrastructure protection.* Retrieved June 1, 2006, from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

Roy-Chowdhury, A., Baras, J., Hadjitheodosiou, M., & Rentz, N. (2005). *Hybrid networks with a space segment—Topology design and security issues*. (Tech. Rep. No. 2005-6.) College Park, MD: University of Maryland, Center for Satellite and Hybrid Communication Networks (CSHCN).

University of Aberdeen. (n.d.). *Satellite reliable multicast transport protocol—A network tool for multimedia file distribution*. Retrieved June 27, 2006, from http://geocast.netvizion.fr/download/sat-rmtp.pdf

U.S. Department of Homeland Security (DHS). (2003). *The national strategy to secure cyberspace.* Washington, DC: Author.

U.S. General Accounting Office (GAO). (2002). *Critical infrastructure protection: Commercial satellite security should be more fully addressed* (Pub. No. GAO-02-781). Washington, DC: Author.

U.S. General Accounting Office (GAO). (2004). *Critical infrastructure protection. Improving information sharing with infrastructure sectors* (Pub. No. GAO-04-780). Washington, DC: Author.

U.S. General Accounting Office (GAO). (2005). *Information security: Emerging cybersecurity issues threaten federal information systems* (Pub. No. GAO-05-231). Washington DC: Author.

Waldrop, E. (2005). Weaponization of outer space: U.S. national policy. *High Frontier: The Journal for Space and Missile Professionals, 1*(3), 35-45.

Wilson, C. (2005). *Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress*. Washington, DC: Library of Congress.

KEY TERMS

Cyber Attack: A computer network attack that involves the use of wireline and/or wireless network connections to gain unauthorized access to computing resources in order to control network operations (Wilson, 2005).

Geostationary or Geosynchronous Earth Orbit (GEO): A satellite constellation with three to five satellites that orbit the earth at altitudes of 35,800 kilometers (km) such as military strategic and tactical relay satellite (MILSTAR) that provides jam-resistant communications services for the U.S. military.

Ground Segment: Terrestrial component in a satellite network that manages and controls satellite operations and processes data for storage and transmission.

IPv6: Developed by the IETF. IPv6 extends IP addresses from 32-bits to 128-bits, thereby overcoming IPv4 address shortages and ensuring continued Internet growth and expansion.

Low Earth Orbit (LEO): Satellite constellations that orbit the earth at altitudes ranging from 500 km to 900 km and support applications such as Internet connectivity.

Medium Earth Orbit (MEO): Mid-sized satellite constellations such as the U.S. Global Positioning System (GPS). GPS satellites maintain orbits at approximately 20,200 km above the earth and provide precise positioning services.

Open Systems Interconnection (OSI) Reference Model: Seven-layer architectural model developed by the International Organization for Standardization (ISO) to describe standardized network operations.

Space Segment: Refers to the artificial satellite and its payload in a satellite network. It enables diverse applications in sectors that include e-government, e-learning, and e-medicine.